



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Synchronizacja [S1Cybez1>SYNCH]

Przedmiot

Kierunek studiów

Cyberbezpieczeństwo

Rok/Semestr

3/5

Studia w zakresie (specjalność)

–

Profil studiów

ogólnoakademicki

Poziom studiów

pierwszego stopnia

Język oferowanego przedmiotu

polski

Forma studiów

stacjonarne

Wymagalność

obieralny

Liczba godzin

Wykład

24

Laboratorium

16

Inne

0

Ćwiczenia

0

Projekty/seminaria

16

Liczba punktów ECTS

4,00

Koordynatorzy

dr inż. Łukasz Matuszewski

lukasz.matuszewski@put.poznan.pl

dr hab. inż. Jakub Nikonowicz prof. PP

jakub.nikonowicz@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z zakresu bezpieczeństwa sieci komputerowych, architektury i protokołów sieciowych, urządzeń sieciowych oraz mechanizmów ochrony infrastruktury ICT. Powinien dysponować umiejętnością analizy zagrożeń w sieciach teleinformatycznych, konfiguracji urządzeń sieciowych oraz monitorowania ruchu sieciowego w celu wykrywania anomalii. W zakresie kompetencji społecznych student powinien prezentować takie postawy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista oraz świadomość etycznych aspektów cyberbezpieczeństwa i ochrony danych.

Cel przedmiotu

1. Przekazanie studentom wiedzy na temat źródeł sygnałów taktowania, metod synchronizacji sieci ICT oraz zagrożeń związanych z manipulacją sygnałami czasu i częstotliwości. 2. Wykształcenie umiejętności projektowania bezpiecznych systemów synchronizacji oraz wykrywania i reagowania na zakłócenia, ataki i awarie w sieciach synchronizacji. 3. Kształtowanie umiejętności pozyskiwania wiedzy o aktualnych rozwiązaniach w zakresie bezpiecznej synchronizacji w systemach teleinformatycznych.

Przedmiotowe efekty uczenia się

Wiedza:

Ma uporządkowaną, szczegółową wiedzę z zakresu teorii telekomunikacji, niezbędną do zrozumienia, analizy i oceny działania metod synchronizacji w kontekście bezpieczeństwa współczesnych sieci ICT. Zna zasady funkcjonowania protokołów synchronizacji czasowej oraz ich wpływ na integralność danych i ochronę przed atakami związanymi z manipulowaniem czasem w sieciach. K1_W05, K1_W15.

Zna podstawowe zasady działania układów synchronizacyjnych na poziomie łącza i sieci, ze szczególnym uwzględnieniem aspektów związanych z zapewnieniem ciągłości usługi, detekcją i przeciwdziałaniem atakom mającym na celu zakłócenie synchronizacji. K1_W09, K1_W10.

Posiada podstawową wiedzę na temat sygnałów taktujących oraz funkcjonowania systemów dystrybucji sygnałów czasu i częstotliwości w sieciach teleinformatycznych. K1_W07.

Umiejętności:

Potrafi określić podstawowe parametry i właściwości sygnałów synchronizacyjnych oraz ocenić ich wpływ na bezpieczeństwo i integralność danych w sieciach teleinformatycznych. K1_U05, K1_U09.

Potrafi zaprojektować podsystem synchronizacji w sieciach przewodowych i bezprzewodowych, uwzględniając mechanizmy ochrony przed atakami mającymi na celu zakłócenie synchronizacji, zapewniając integralność i dostępność transmisji. K1_U02, K1_U08, K1_U11.

Potrafi zapewnić synchronizację sieci, nadzorować ich pracę oraz wykorzystywać technologie synchronizacyjne, które umożliwiają bezpieczne przesyłanie danych. K1_U03 .

Kompetencje społeczne:

Dostrzega zmiany wynikające z postępu technologicznego i rozumie potrzebę śledzenia nowych standardów dotyczących synchronizacji i ochrony sieci teleinformatycznych. K1_K01.

Ma poczucie odpowiedzialności za projektowane systemy informatyczne, zdaje sobie sprawę z zagrożeń społecznych związanych z ich niewłaściwym zaprojektowaniem lub realizacją, szczególnie w kontekście ochrony prywatności i integralności danych. K1_K05.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład:

Weryfikacja efektów kształcenia odbywa się poprzez egzamin w formie testu wielokrotnego wyboru. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania, zostaną udostępnione studentom za pośrednictwem uczelnianej platformy nauczania zdalnego. Do uzyskania oceny 3.0 niezbędne jest zdobycie ponad połowy możliwych punktów.

Laboratorium:

Ocena efektów kształcenia realizowana jest poprzez:

1. Ocenianie ciągłe - każdorazowa weryfikacja wiedzy poprzez odpowiedzi ustne na pytania zadawane w trakcie wykonywania ćwiczeń laboratoryjnych.
2. Sprawozdania z wykonanych ćwiczeń, uwzględniające analizę poprawności synchronizacji i identyfikację potencjalnych zagrożeń.
3. Ocena uzyskana ze sprawdzianu podsumowującego ćwiczenia, sprawdzającego zarówno wiedzę teoretyczną, jak i praktyczne umiejętności konfiguracji i analizy systemów synchronizacji.
4. Punkty dodatkowe za aktywność podczas zajęć laboratoryjnych, np. za inicjatywę w rozwiązywaniu problemów związanych z bezpieczeństwem synchronizacji w sieciach ICT.

Projekt:

1. Ocena raportu projektowego: każdy projekt powinien być dostarczony w formie raportu zawierającego pełną dokumentację projektu.
2. Prezentacja projektu: prezentacja powinna obejmować główne cele projektu, zastosowaną metodologię, wyniki oraz wnioski, a także uzasadnienie wyborów technicznych i rozwiązań.
3. Demonstrowanie działania projektu: uruchomienie aplikacji, prezentując implementację algorytmu, czy demonstrując działanie systemu w przypadku projektów technicznych.

Udział kryteriów oceny w ocenie końcowej:

1. Funkcjonalność i jakość techniczna (40%) - działanie projektu, wydajność, poprawność implementacji, optymalizacja.
2. Jakość dokumentacji (30%) - pełność, jasność, struktura raportu, poprawność merytoryczna.
3. Jakość prezentacji (30%) - jasne przedstawienie projektu, odpowiedzi na pytania, umiejętność

komunikacji, estetyka prezentacji.

Zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Przedmiot wprowadza kluczowe zagadnienia związane z rolą synchronizacji w zapewnianiu spójności operacyjnej w sieciach ICT, wpływając bezpośrednio na integralność i dostępność systemów. Program obejmuje różnorodne techniki synchronizacji oraz ich znaczenie w kontekście ochrony infrastruktury ICT. Istotnym elementem kursu są źródła sygnałów czasu i częstotliwości, takie jak GNSS, PTP, SyncE, White Rabbit oraz Open Time Protocol, które są analizowane pod kątem podatności na ataki i zakłócenia. W ramach kursu omawiane są również wyzwania związane z synchronizacją w sieciach 5G oraz mechanizmami synchronizacji over-the-air.

Dzięki dokładnemu zrozumieniu tych technologii, studenci uczą się identyfikować i przeciwdziałać potencjalnym zagrożeniom. Zdobyczą umiejętności w zakresie konfiguracji i zabezpieczania urządzeń synchronizacyjnych oraz praktycznej analizy logów w celu wykrywania nietypowych zdarzeń.

Kurs kończy się projektem dotyczącym detekcji anomalii oraz testem wiedzy, co pozwala na praktyczne zastosowanie zdobytej wiedzy i umiejętności.

Tematyka zajęć

Wykłady:

1. Wprowadzenie do synchronizacji i jej rola w bezpieczeństwie sieci ICT (1 godz.).
2. Pętla synchronizacji fazy dla sygnałów ciągłych i dyskretnych (4 godz.).
3. Model sygnału synchronizacji, jego parametry i zagrożenia związane z manipulacją sygnałem (4 godz.).
4. Źródła sygnałów czasu i częstotliwości oraz ich podatności na ataki (4 godz.).
5. Ocena jakości synchronizacji urządzeń i wykrywanie anomalii bezpieczeństwa (4 godz.).
6. Synchronizacja oparta na sieci Ethernet: SyncE, PTP (2 godz.).
7. Nowe technologie synchronizacji White Rabbit, OTP (2 godz.).
8. Synchronizacja w sieciach 5G - wyzwania i zabezpieczenia (2 godz.).
9. Zaliczenie - test wielokrotnego wyboru (1 godz.).

Laboratorium:

1. Źródła sygnału taktowania - konfiguracja i zabezpieczenia (4 godz.).
2. Źródła sygnału synchronizacji - analiza podatności na zakłócenia i ataki (4 godz.).
3. Pomiar jakości synchronizacji urządzenia i wykrywanie anomalii bezpieczeństwa (6 godz.).
4. Zaliczenie laboratorium (2 godz.).

Projekt:

- System detekcji anomalii w NTP - analiza logów, wykrywanie spoofingu i ataków na synchronizację (8 godz.).
- Klasyfikacja anomalii w sygnałach czasu - model uczenia maszynowego do wykrywania nietypowych zdarzeń (8 godz.).

Metody dydaktyczne

Wykłady:

1. Prezentacja multimedialna: wykładowca przedstawia materiał za pomocą slajdów, uzupełnionych o zdjęcia, filmy i inne elementy wizualne, rzeczywistych urządzeń/pomiarów systemów synchronizacji.
2. Wykład interaktywny: wykładowca angażuje studentów w dyskusję, zadaje pytania i zachęca do dzielenia się własnymi przemyśleniami, wspomagając lepsze zrozumienie materiału i rozwijanie umiejętności krytycznego myślenia.
3. Studium przypadku: wykładowca omawia konkretny przykład, analizując problem i proponując rozwiązania. To pozwala na zastosowanie wiedzy teoretycznej w praktyce.

Laboratorium:

1. Symulacje: Studenci pracują z programami komputerowymi, które imitują rzeczywiste sytuacje.
2. Ćwiczenia praktyczne: studenci wykonują zadania pod okiem prowadzącego, ucząc się praktycznego wykorzystania wiedzy.
3. Praca w grupach: studenci współpracują nad rozwiązaniem problemu, dzieląc się wiedzą i rozwijając umiejętności komunikacji i pracy zespołowej.

Projekt:

1. Praca nad projektem: studenci realizują projekt pod kierunkiem opiekuna, zdobywając doświadczenie

w planowaniu, organizacji i realizacji zadań, rozwijając umiejętności menedżerskie i organizacyjne.
2. Prezentacja projektu: studenci prezentują wyniki swojej pracy, rozwijając zdolności komunikacji i autoprezentacji.

Literatura

Podstawowa:

- [1] ETSI, "Synchronization in telecommunication networks," ETSI TS 102 031, 2018.
- [2] IEEE, "IEEE Standard for Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," IEEE Std 1588-2008, 2008.
- [3] ITU-T, "Timing and synchronization in packet networks," ITU-T Rec. G.8272, 2016.

Uzupełniająca:

- 4] S. Galli and L. Musumeci, "Synchronization of Digital Telecommunication Networks," Academic Press, 2003.
- [5] L. Shu and M. Youssef, "Time Synchronization in Wireless Sensor Networks," Springer, 2012.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	116	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	56	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwίων/egzaminu, wykonanie projektu)	60	2,00